PCT/EP2004/051153

BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

REC'D 26 AUG 2004
WIPO PCT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 27 610.6

Anmeldetag: 18. Juni 2003

Anmelder/Inhaber: Siemens Aktiengesellschaft, 80333 München/DE

Bezeichnung: Mechanismus zur sicheren Konfiguration von mobilen Endgeräten

IPC: H 04 Q 7/38

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 08. Juli 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Schäfer

A 9161
06/00
EDV-L

BEST AVAILABLE COPY

1. Welches technische Problem soll durch die Erfindung gelöst werden?

Mobile Endgeraete erhalten beim Netzzugang eine Reihe von Konfigurationsparametern. Der Mechanismus ueber den diese Parameter bereitgestellt werden, haengt sehr stark vom Anwendungsscenario ab:

Fuer mobile Endgeraete, die sich in einem lokalen Netzwerk (z.b. Hostspot) anmelden, besteht diese Moeglichkeit oft nicht, da weder PPP noch VPNs benutzt werden. Erfolgt kein Schutz der Konfigurationsdaten, so besteht die Moeglichkeit fuer einen Angreifer sowohl dem Endgeraet als auch dem Netzwerk Schaden zuzufuegen. Eine Beschreibung der Sicherheitsbedrohungen ist unter anderem in [THREATS] zu finden.

Ziel dieser Erfindung ist es daher einen Mechanismus zu definieren, der es mobilen Endgeraeten erlaubt Konfigurationsdaten gesichert zu erhalten.

2. Wie wurde dieses Problem bisher gelöst?

Abbildung 1 zeigt die Vielzahl der Protokolle, die bei einem Netzwerkzugang ausgefuehrt werden. Fuer diesen Mechanismus sind speziell die Bausteine (2) und (3) von Interesse. Das Zusammenspiel dieser [illegible] wird in Abschnitt 5 erlaeutert.

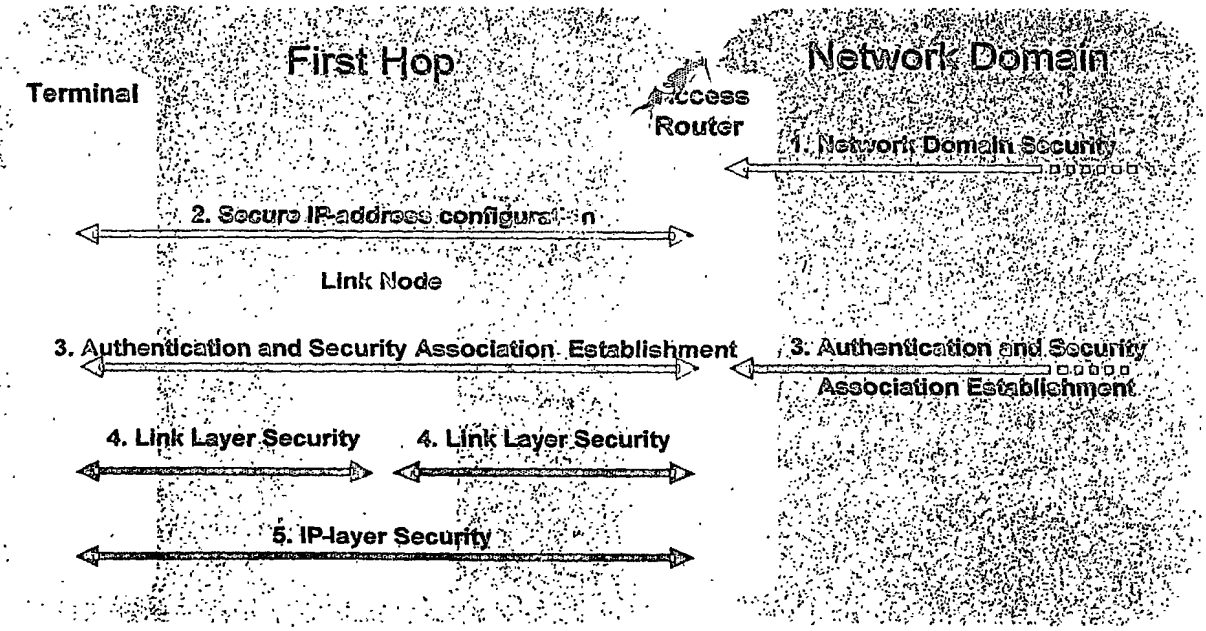


Abbildung 2: Protokollinteraktion beim Netwerkzugang

Der Mechanismus ueber den diese Parameter bereitgestellt werden, haengt sehr stark vom Anwendungsscenario ab:

- In Firmennetzwerken werden Konfigurationsparameter entweder statisch konfiguriert oder dynamisch durch DHCP [DHCPv6] oder [RFC2131] erhalten. Meist findet dabei keine Schutz dieser Protokolle statt. DHCP bietet jedoch die Moeglichkeit diese Nachrichten durch einen vorab ausgehandelten Schluessel zu sichern (siehe (RFC3118]).

- Fuer den Zugang zu einem Internet Service Provide wird nahezu ausschliesslich PPP (oder auch eine Variation PPPoE) benutzt, um diese Konfigurationsdaten an das Endgeraet zu transportieren.

- Fuer den VPN Zugang zu einem Netzwerk wurden in der Vergangenheit zwei Protokolle verwendet, um diese Konfigurationsdaten geschuetzt zu transportieren: ModeConfig und DHCP ([Ric03], [Kiv03], [Duk02], [DP01]). Beide Verfahren wurden in das Authentifikations und Schluesselaushandlungsprotokoll IKE bzw. IKEv2 integriert.

Um sichere Konfigurationsdaten zwischen dem Netzwerk und dem mobile Endgeraet zu ermoeglichen, wurden in der Vergangenheit unterschiedliche Methoden benutzt. Diese Methoden lassen sich grob in drei Gruppen aufteilen:

- Erweiterungen zu DHCP

Um DHCP Nachrichten im mobilen Umfeld zu schuetzen wurden eine Reihe von Erweiterungen zum DHCP Protokoll vorgeschlagen (z.b. [MD+00], [MG+00], [ML00] [Gup03]). Diese Vorschlaege sollen es einem Endgeraet erlauben sich dynamisch im Netzwerk eine Sicherheitsbeziehung mit dem DHCP Server aufzubauen.

- EAP Methoden Erweiterungen

Eine kuerzlich vorgeschlagene EAP methode (EAP-IKEv2 [TK03]) erlaubt es IKEv2 [IKEv2] wiederzuverwenden. Als ein Nebeneffekt besteht in IKEv2 die Moeglichkeit Konfigurationsdaten geschuetzt zu uebertragen. Zur Diskussion stehen dabei zwei Methoden: Modeconfig ([Duk02], [DP01]) und ein auf DHCP basierender Ansatz ([Ric03], [Kiv03]).

- Bootstrapping Methode

In der Arbeit in der PANA IETF Arbeitsgruppe wurde an einem Protokollvorschlag gearbeitet, mit dem die initiale Netzwerkauthentifikation (mittles EAP) und die Bereitstellung einer Sicherheitsverbindung mit dem DHCP server ermoeglicht wird. Der Vorteil dieses Verfahrens liegt in der Trennung zwischen Netzwerkauthentifikation und der Sicherung der DHCP Nachrichten. Das DHCP Protokoll muss dabei nicht veraendert werden.

3. In welcher Weise löst die Erfindung das angegebene technische Problem (Vorteile)?

Die vorgeschlagenenen standard Konfigurationsprotokolle (DHCP/Modeconfig) ([Ric03],[Kiv03], [Duk02], [DP01]) werden benutzt um ein Endgeraet zu konfiguriert. Dies geschieht in einer Art und Weise, die in diesem Umfeld noch nicht existiert. Die Sicherung dieser Protokolle erfolgt durch die von der vorangegangenen EAP-basierten Netwerkauthentifikationsmechanismen bereitgestellten Schluessel.

4. Worin liegt der erfinderische Schritt?

Verwendung von existierenden Konfigurationsprotokollen (DHCP/Modeconfig) geschuetzt durch die vorangegangene Netzwerkzugangsauthentifikation.

Im Speziellen sollen Mechanismen zur sicheren Uebertragung von Konfigurationsdaten fuer

- PEAP [PEAP]
- TTLS [TTLS]
- PANA [PANA] oder als
- eigene EAP selbst. Der Schutz dieser EAP Konfigurationsnachrichten erfolgt dabei entweder ueber existierende Tunneling-Methoden (z.b. PEAP, TTLS, etc.) oder durch EAP interne Schutzmechanismen (z.b. Protected TLV [HP+03]). Dabei ist es ebenfalls moeglich [GS03] als Container zu verwenden um die Konfigurationsdaten zu transportieren.

definiert werden.

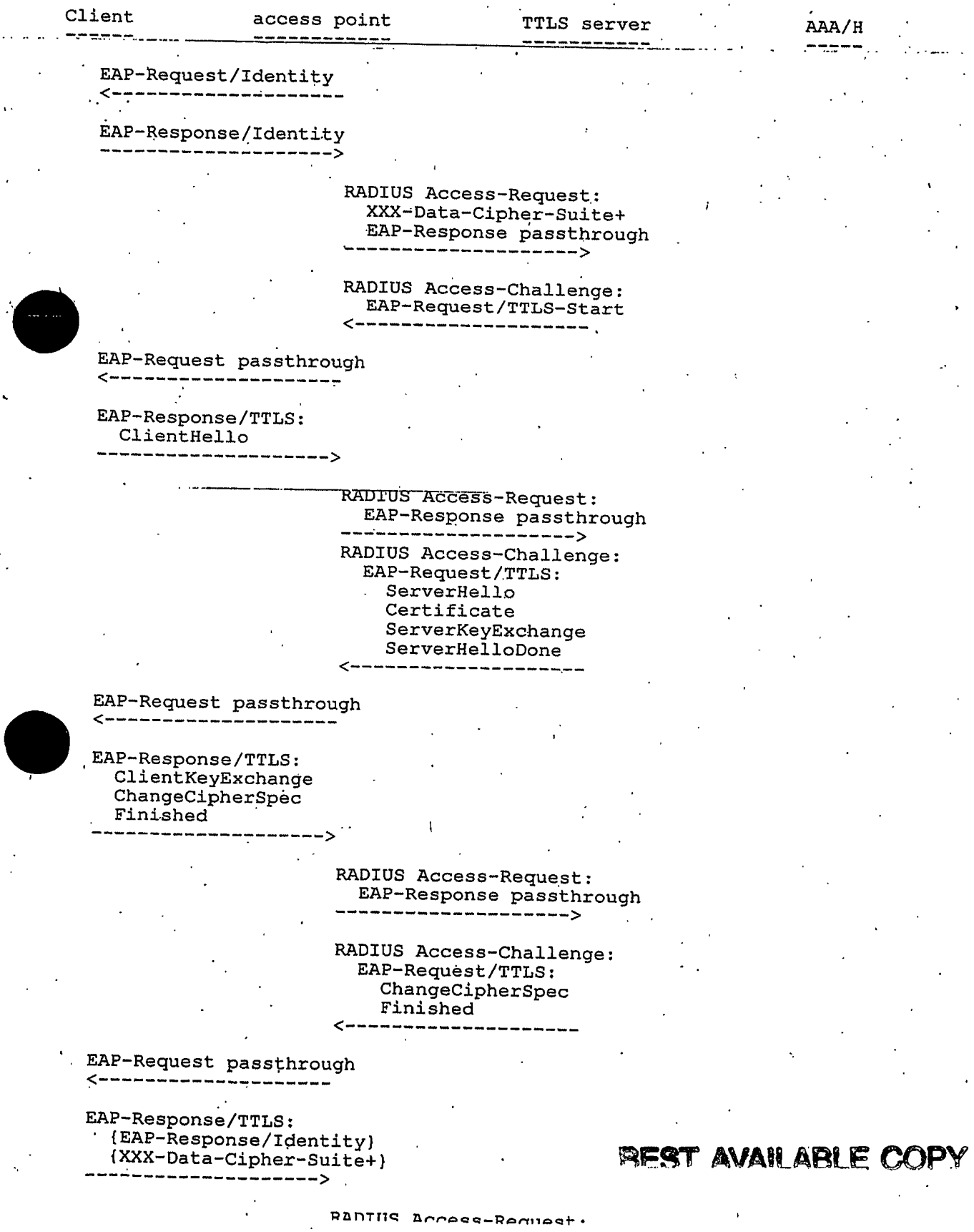
5. Ausführungsbeispiel

Der nachfolgende Nachrichtenfluss wurde aus Abschnitt 13.2 von [TTLS] entnommen und angepasst. Das Beispiel zeigt den Aufbau eines TLS tunnels (einseitig Authentifikation; Server zu Client) mit anschliessender EAP/MD5-Challenge Authentifikation (einseitige Client zu Server Authentifikation).

Fuer dieses Dokument ist die Uebertraung der Konfigurationsdaten nach Ende der Authentifikation entscheidend. In diesem Beispiel wird [Duk02] verwendet um den Client die Moeglichkeit zu geben, Konfigurationsdaten mittels CFG_REQUEST anzufordern und ueber CFG_REPLY zu erhalten. Die Verwendung von DHCP ist dabei bis auf die Nachrichtenformate gleich

Die Uebertragung der Konfigurationsdaten erfolgt dabei gesichert durch den TLS tunnel. Im Beispiel nicht enthalten ist die Kommunikation zwischen dem TTLS server und dem Knoten, der die Konfigurationsdaten bereistellt (z.b. DHCP oder auch LDAP server).

Anmerkung: Die Konfigurationsdaten koennen auch unmittelbar nach dem Ende der Authentifikation (z.b. mit der EAP success Nachricht) and das Endgeraet geschickt werden.



BEST AVAILABLE COPY

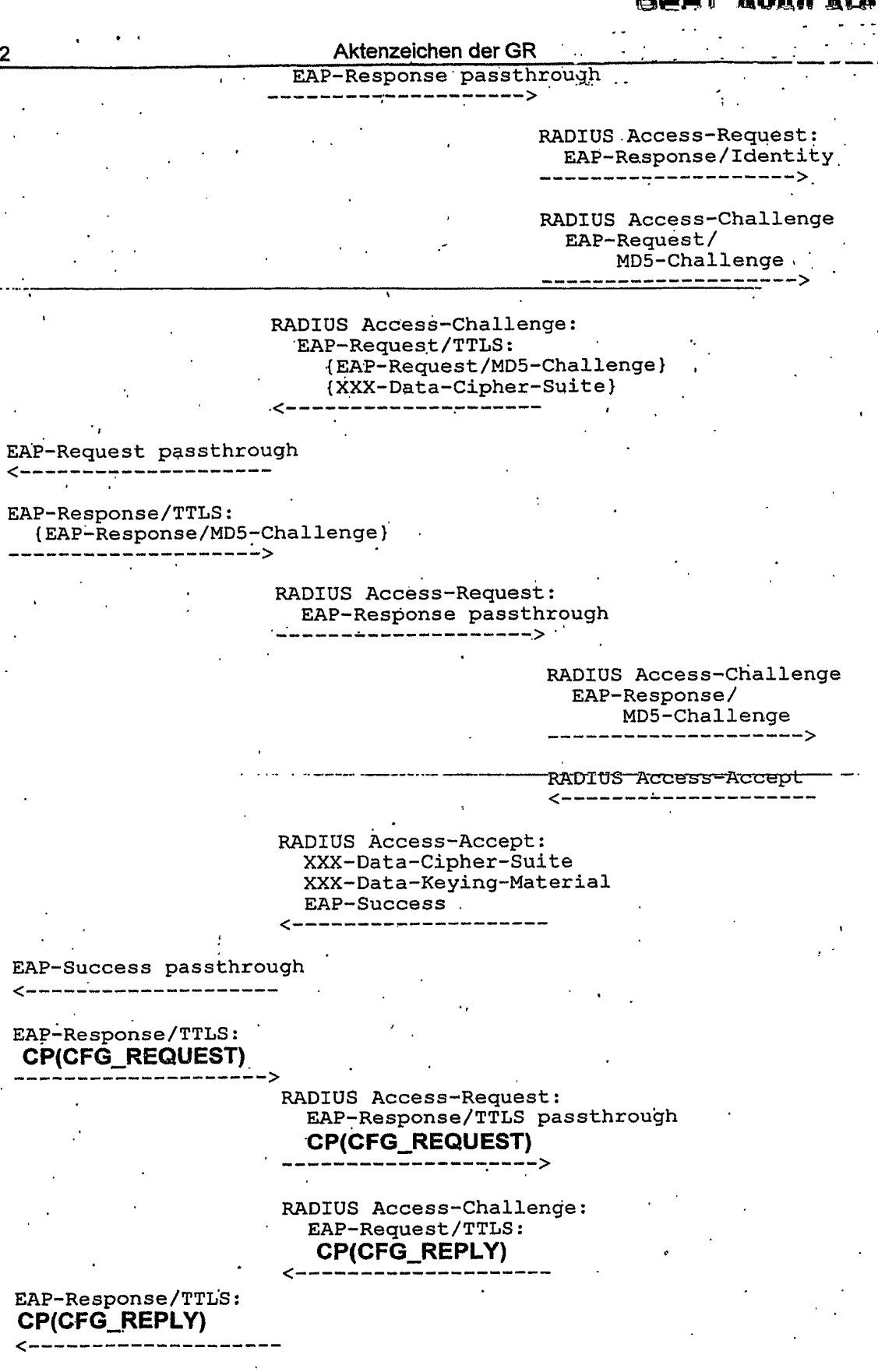
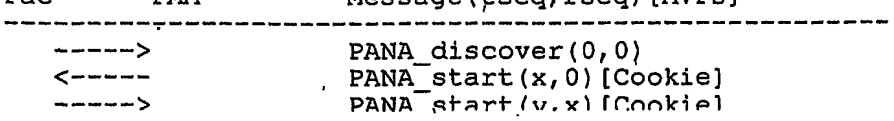


Abbildung 2: EAP-TTLS Protokoll mit Address-Konfiguration

Als weiteres Ausfuehrungsbeispiel wird der Nachrichtenfluss in PANA dargestellt:



BEST AVAILABLE COPY


```
      <-----          PANA_auth(x+1,y)[EAP{Request}]
      ----->          PANA_auth(y+1,x+1)[EAP{Response}]

      <-----          PANA_auth(x+2,y+1)[EAP{Request}]
      ----->          PANA_auth(y+2,x+2)[EAP{Response}]

-- PANA SA Established --

      <-----          PANA_success(x+3,y+2)                  // F-flag set
                      [EAP{Success}, Device-Id, Data-Protection, MAC]
      ----->          PANA_success_ack(y+3,x+3)
                      [Device-Id, Data-Protection, CP(CFG_REQUEST), MAC]
                      // F-flag set
      <-----          PANA_msg(x+4,y+3)
                      [CP(CFG_REQUEST), MAC]
```

Abbildung 3: PANA Protokoll mit Address-Konfiguration

In Abbildung 3 wird das PANA Protokoll mit seinen Nachrichtenfluessen dargestellt. Die Erweiterungen zum PANA Protokoll sind minimal und beschraenken sich auf die Payloads zum Transport der Adresskonfigurationsnachrichten (DHCP/ModeConfig). In Abbildung 3 wurde das beispielhaft die Konfigurationspayloads aus [Duk02] verwendet. Die Anfrage und die Antwort zum Erhalt der [illegible]gurationsdaten wird durch den MAC-Payload, der durch eine Keyed Message Digest Funktion [illegible]ert wird geschuetzt. Die benoetigten Schluessel und Sicherheitsparameter werden durch die [illegible]A Security Association (SA) bereitgestellt, die durch die EAP Authentifikation erzeugt wurden.

Referenzen:

[GS03] M. Grayson and J. Salowey: "EAP Authorization", Internet-Draft, (work in progress), March 2003.

[TK03] H. Tschofenig, D. Kroeselberg: "EAP IKEv2 Method", Internet-Draft, (work in progress), April 2003.

[RFC2409] D. Harkins, D. Carrel: "The Internet Key Exchange (IKE)", RFC 2409, November, 1998.

[Ric03] M. Richardson: "A method for configuration of IPsec clients using DHCP", Internet-Draft, (work in progress), Februrary, 2003.

[Duk02] D. Dukes: "Configuration payload", Internet-Draft, (work in progress), December, 2002.

ModeConfig und DHCP

[illegible]1] D. Dukes and R. Pereira: "The ISAKMP Configuration Method", Internet-Draft, (expired), September 2001.

[Kiv03] T. Kivinen: "DHCP over IKE", Internet-Draft, (work in progress), April 2003.

[DHCPv6] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Internet-Draft, (work in progress), November, 2002.

[RFC2131] R. Droms: "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3118] R. Droms and W. Arbaugh: "Authentication for DHCP Messages", RFC 3118, June 2001.

[IKE] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[IKEv2] C. Kaufman: "Internet Key Exchange (IKEv2) Protocol", Internet-Draft, (work in progress), April, 2003.

[HP+03] T. Hiller, A. Palekar, G. Zorn: "A Container Type for the Extensible Authentication Protocol (EAP)", Internet-Draft, (work in progress), May, 2003.

[PEAP] Andersson, H., et al. "Protected EAP Protocol", Internet draft (work in progress), February 2002.

[TTLS] P. Funk, S. Blake-Wilson: "EAP Tunneled TLS Authentication Protocol", Internet draft (work in progress), February 2002.

[PANA] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig and A. Yegin: "Protocol for Carrying Authentication for Network Access (PANA)", Internet-Draft, (work in progress), March, 2003.

[THREATS] N. Prigent, J. Marchand, F. Dupont, B. Cousin, M. Laurent-Maknavicius, J. Bournelle: "DHCPv6 Threats", Internet-Draft, (expired), May 2001.

[MD+00] McAuley, A., Das, S., Madhani, S., Baba, S., Shobatake, Y.: "Dynamic Registration and Configuration Protocol (DRCP)", <draft-itsumo-drcp-01.txt>, (expired), July, 2000.

[MG+00] Mukherjee, B., Gage, B., Liu, Y., Melzer, J.: "Extensions to DHCP for Roaming Users", <draft-mukherjee-dhc-dhcproam-00.txt>, (expired), October, 2000.

[ML00] Medvinsky, S., Lalwaney, P.: "Kerberos V Authentication Mode for Uninitialized Clients", <draft-smedvinsky-dhc-kerbauth-01.txt>, (expired), September 2000.

[...03] V. Gupta: "Flexible Authentication for DHCP Messages", Internet-Draft, (work in progress), February, 2003

Patentanspruch

Verfahren, bei dem ein mobiles Endgerät gesichert Konfigurationsdaten erhält.